RECEIVED
2 2 JAN 2004
| WIPO | PCT |

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.
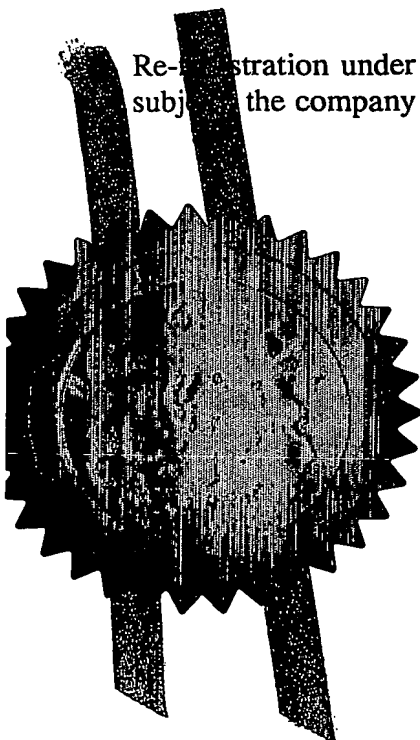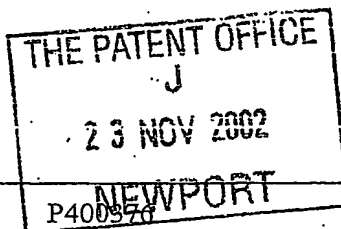
Signed

Dated   13 January 2004

BEST AVAILABLE COPY

ts Form 1/77

Pate \ct 1977
(Rule ..)

The
Patent
Office

1/77

Request for grant of a patent
(see the notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)

THE PATENT OFFICE
J
2 3 NOV 2002
NEWPORT
P40039?0

The Patent Office

Cardiff Road, Newport
South Wales NP9 1RH

25NOV02 E765890-2 D02835
PO1/7700 0.00-0227396.9

1.	Your reference		
2.	Patent application number *(The Patent Office will fill in this part)*	**0227396.9**	2 3 NOV 2002

3.   Full name, address and postcode of the or of each applicant *(underline all surnames)*

Maxsi Limited
Hadrian House
Higham Place
Newcastle upon Tyne NE1 8AF

Patents ADP number *(if you know it)*

If the applicant is a corporate body, give the country/state of its incorporation

England   0551 249 3 001

4.   Title of the invention

METHOD OF ANALYSING ACTIVITY IN A
NETWORK OF INTERCONNECTED COMPUTERS

5.   Name of your agent *(if you have one)*

"Address for service" in the United Kingdom to which all correspondence should be sent *(including the postcode)*

Patents ADP number *(if you know it)*

URQUHART-DYKES & LORD
ST NICHOLAS CHAMBERS
AMEN CORNER
NEWCASTLE UPON TYNE
NE1 1PE

00001644019

6.   If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications and *(if you know it)* the or each application number

Country	Priority application number *(If you know it)*	Date of filing *(day/month year)*

7.   If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application

Number of earlier application	Date of filing *(day/month/year)*

8.   Is a statement of inventorship and or right to grant of a patent required in support of this request? *(Answer "Yes" if:)*
a) any applicant named in part 3 is not an inventor, or
b) there is an inventor who is not named as an applicant, or
c) any named applicant is a corporate body; see note (d)

YES

9. Enter the number of sheets for any of the
following items you are filing with this form.
· Do not count copies of the same document

Continuation sheets of this form

Description	8
Claim(s)	3
Abstract	
Drawing(s)	1

10 If you are also filing any of the following
items state how many against each item:

Priority documents

Translation of priority documents

Statement of inventorship and right
to grant of a patent *(patents form 7/77)*

Request for preliminary examination
and search *(patents form 9/77)*

Request for substantive examination
(patents form 10/77)

Any other documents
(please specify)

11
I/We request the grant of a patent on the basis of this application.
Signature   Date   21/11/02

URQUHART-DYKES & LORD

12 Name and daytime telephone number of
person to contact in the United Kingdom

Martin Vinsome - 0191 2618573

Warning

After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom , Section 23 of the Patent Act 1977 stops you from applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked.

Notes

a) if you need help to fill in this form or you have any questions, please contact the Patent Office on 0645 500505.

b) Write your answers in capital letters using black ink or you may type them.

c) If there is not enough space for all the relevant details on any part of this form, please continue on a separate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.

d) If you have answered "Yes" Patents Form 7/77 will need to be filed

e) Once you have filled in the form you must remember to sign and date it.

f) For details of the fee and ways to pay please contact the Patent Office.

METHOD OF ANALYSING ACTIVITY IN A NETWORK OF INTERCONNECTED COMPUTERS

The present invention relates to a method of analysing activity in a network of interconnected computers, and relates particularly, but not exclusively, to a method of analysing Internet website user activity.

In recent years, use of the Internet, also known as the World Wide Web, has grown enormously. Modern Internet websites can be extremely sophisticated and offer a wide range of services and information for the user, as well as offering goods and services for sale.

As a result of this, there has been an increasing demand from website proprietors to be able to analyse how the websites are being used, so that they can constantly audit and improve their websites. For example, a proprietor may wish to know for how long and by how many users its website has been accessed, or may wish to acquire more sophisticated information such as which link to the website has generated the most business or income in a particular period.

One known method of website activity analysis is known as log file analysis. Websites are displayed on user's computers by means of software known as browser software, usually as a combination of text and graphics, although the website itself consists of computer codes stored on a server computer (known as the web server) located remotely from the user's computer. When a user sends a request for a website to the Internet, the web server sends the website, via the Internet, to the user's browser.

Most servers are capable of generating log files which are stored on the web server and accumulate simple data such as the number of times the pages of the website have been requested. In order for the website proprietor to obtain information about traffic involving the website, the log file must be downloaded to the proprietor's computer and analysed by software running on this computer.

Log file analysis suffers from a number of disadvantages. Firstly, log files are often quite large and therefore take a considerable amount of time to download and require large amounts of disk space. As a result of this, by the time a log file is downloaded and analysed, it is likely that further traffic will have occurred on the website, and the log file will therefore represent out-of-date information.

Furthermore, log file analysis does not take caching into account. A cache is an intermediate point in the Internet, between the user and the web server, at which some of the website code is stored, for example text or graphics files. This reduces traffic on the Internet, and speeds up user access to websites, since some of the code for a particular website may already be stored at an intermediate point and may therefore not need to be sent from the web server. As a result of this, a website cannot record data relating to the access of cached information, and will therefore provide an inaccurate representation of website user activity.

Another prior art method of website activity analysis is known as tagging. Tagging comprises adding a portion of computer code, usually in the JavaScript programming language, to the main website code such that when the browser software of the user's computer processes the website code, it also activates the tag. The tag, when activated, then acquires information about use of the website to which it is attached, and uploads

this information to a separate server, called an analysis server, at which analysis of traffic on the website can be carried out. The analysis server is pre-programmed to accept certain data types acquired by the tag, and stores the data accordingly. The website proprietor can then access the website traffic data stored on the analysis server. In this way, the method of tagging is more up to date than log file analysis, and is also independent of caching, as the actual data acquisition takes place at the user's computer.

However, tagging suffers from the drawback that the tag can only record data that the analysis server is pre-programmed to accept, which makes this method of data acquisition inherently inflexible. For example, if a new type of data not included in the types the tag is pre-programmed to look for is required, both the analysis server and the web server must be reprogrammed. As a result, access to the analysis server software is required, as a result of which the security of the analysis server may be compromised.

Preferred embodiments of the present invention seek to overcome the above disadvantages of the prior art.

According to an aspect of the present invention, there is provided a method of acquiring data relating to website activity in a network of interconnected computers, the method comprising:-

defining, at a first computer, a first computer code defining a set of data parameters, the values of which are to be acquired from a second computer; and

supplying to said second computer, in response to a request for web page data sent to said first computer from said second computer, web page data together with said first computer code;

wherein said first computer code is adapted to acquire from said second computer the values of said set of data parameters and provide said values, together with data identifying said parameters, to a third computer.

This provides the advantage that the person setting up or altering web page data can decide the parameters of which data is to be collected, and the data identifying said parameters enables the data to be analysed at the third computer without the necessity of reprogramming both the first and third computers.

Said data identifying said parameters may represent the type and/or format and/or description of said data values.

The method may further comprise the step of supplying a second computer code to said second computer, wherein said second computer code is adapted to encrypt said data values and/or said data identifying said parameters.

By supplying a second computer code adapted to be executed at the second computer to encrypt data sent from said second computer, this provides the advantage of making data transmitted by the second computer more difficult to intercept, since it can be encrypted before it is sent to a location remote from the second computer.

According to another aspect of the present invention, there is provided a method of monitoring website activity in a network of interconnected computers, the method comprising:-

receiving at a first computer, in response to a request for web page data sent from a second computer to a third computer, a set of data values, representing values of a set of parameters

relating to said second computer, from said second computer together with data identifying said parameters; and

analysing said data values using said data identifying said parameters.

The data identifying said parameters may represent the type and/or format and/or description of said data values.

The method may further comprise the step of providing a second computer code to said second computer, wherein said second computer code is adapted to encrypt data supplied by said second computer.

According to a further aspect of the present invention, there is provided a computer program product comprising:-

a first computer code to be supplied by a first computer and adapted to define a set of data parameters, the values of which are to be acquired from a second computer; and

a second computer code defining data identifying said parameters;

wherein said first and second computer codes are adapted to be supplied to said second computer in response to a request from said second computer for web page data from said first computer and to provide said data values together with said data identifying said parameters to a third computer.

The computer program product may further comprise a third computer code adapted to encrypt data send from said second computer.

A preferred embodiment of the invention will now be described, by way of example only and not in any limitative sense, with reference to the accompanying drawing in which:-

Fig 1 is a schematic representation illustrating a network of interconnected computers executing a process embodying the present invention.

Referring to Figure 1, a user operating a personal computer 1 logs on to the Internet 2 which physically comprises a plurality of computers 3 known as servers (only one of which is shown in Figure 1) connected by optical fibres and/or telephone lines and, using browser software running on computer 2, requests a page from a website from the Internet by entering the appropriate URL (Universal Resource Locator) of the website. This request 4 is passed to the Internet, which then routes the request 4 to a server 3 (known as a web server) which stores the computer code of the requested website.

The web server 3 then sends the requested website data 5 to the user computer 1 via the internet 2. The code of the requested website 5 contains what is known as a JavaScript tag which, as will be familiar to persons skilled in the art, is a portion of code written in the JavaScript programming language added to the main code of the website, the function of which will be described in greater detail below.

The browser software running on the user computer 1 interprets the website code and displays the website to the user. At the same time, the browser software activates the tag which, when activated, compiles a set of data containing information about the user's activity on the website. The type of data being compiled is preprogrammed into the tag at the web server 3 and, for example, may comprise information relating to which hyperlinks the user accesses, up to more complex information

such as how the user arrived at the website, and so on. The information obtained by the tag may represent a variety of different things, and may also be in several different formats. For this reason, the tag also compiles a set of data containing information about the type and format of the data collected as an aid to interpreting the compiled data.

The tag, when activated, also sends a request 6 for a program module via the Internet 2 to an analysis server 7, i.e. a computer at which the data compiled by the tag is to be analysed, or to the web server 3. The analysis server 7, which may be the computer of the website proprietor or may be the computer of a third party carrying out data analysis on behalf of the website proprietor, or the web server 3, then sends the program module 8 to the user computer 1, via the Internet 2. This program module 8 contains computer code which is able to encrypt all of the data obtained by the tag. The encrypted tag data, and encrypted data type and format information 9, is then sent automatically to the analysis server 7 via the Internet 2.

At the analysis server 7, the type and format data is de-encrypted and used to operate software stored on the analysis server 7 that stores and interprets each type of activity data into a separate data field. In this way, any type of data format from any application can be obtained by the tag, and the analysis server will be instructed how to deal with it automatically.

A second user 10, who is most likely the website proprietor, can now download the analysed data 11 from the analysis server 7. This can be done in the form of directly sent data 11, or indirect data 12 via the Internet 2, in which case the data 12 is likely to be encrypted.

It will be appreciated by persons skilled in the art that the above embodiment has been described by way of example only and not in any limitative sense, and various alterations and modifications are possible without departure from the scope of the invention as defined by the appended claims.

CLAIMS

1. A method of acquiring data relating to website activity in a network of interconnected computers, the method comprising:-

defining, at a first computer, a first computer code defining a set of data parameters, the values of which are to be acquired from a second computer; and

supplying to said second computer, in response to a request for web page data sent to said first computer from said second computer, web page data together with said first computer code;

wherein said first computer code is adapted to acquire from said second computer the values of said set of data parameters and provide said values, together with data identifying said parameters, to a third computer.

2. A method according to claim 1, wherein said data identifying said parameters represents the type and/or format and/or description of said data values.

3. a method according to claim 1 or 2, further comprising the step of supplying a second computer code to said second computer, wherein said second computer code is adapted to encrypt said data values and/or said data identifying said parameters.

4. A method of acquiring data relating to website activity in a network of interconnected computers, the method substantially as hereinbefore described with reference to the accompanying drawing.
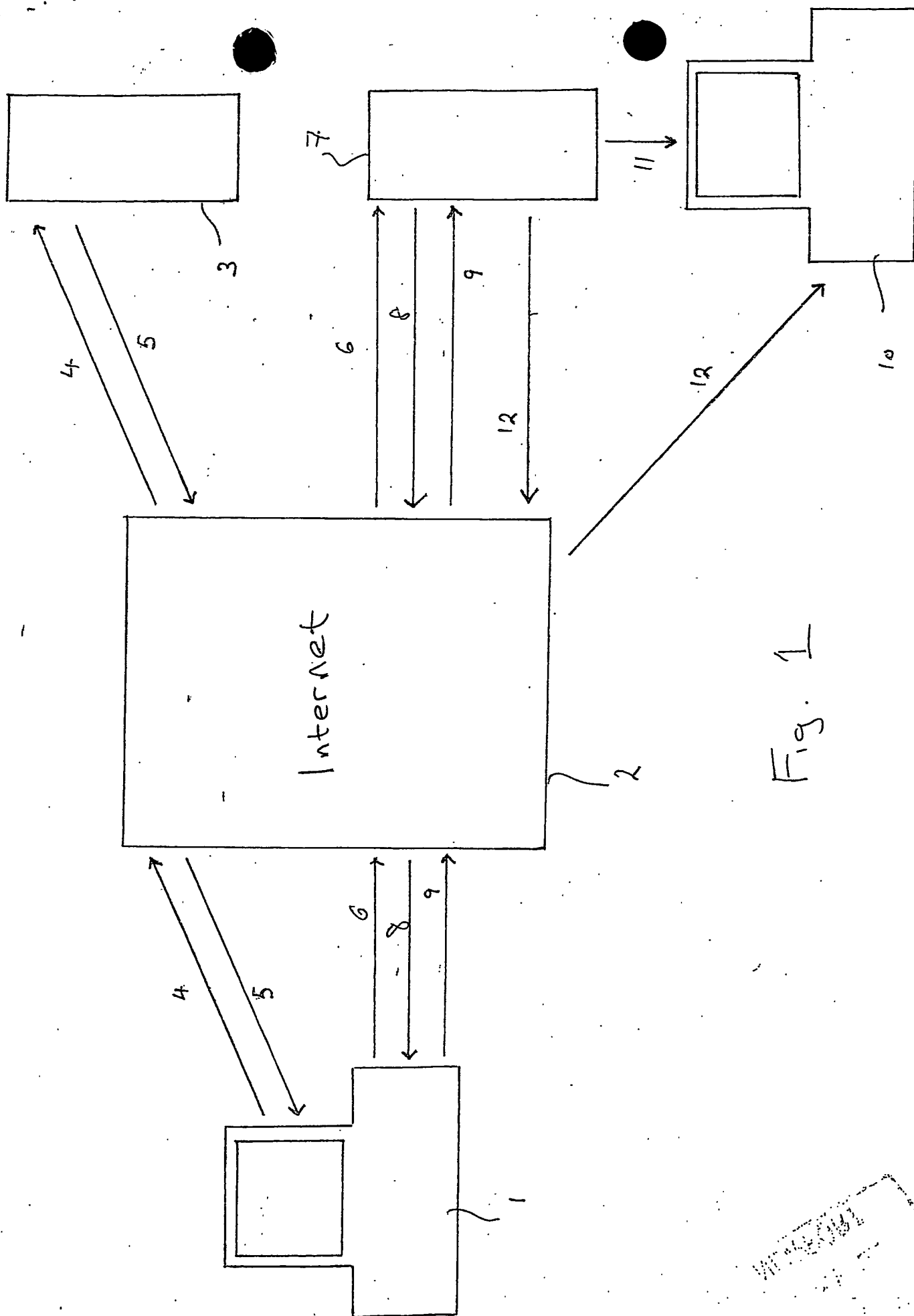
5. A method of monitoring website activity in a network of interconnected computers, the method comprising:-

receiving at a first computer, in response to a request for web page data sent from a second computer to a third computer, a set of data values, representing values of a set of parameters relating to said second computer, from said second computer together with data identifying said parameters; and

analysing said data values using said data identifying said parameters.

6. A method according to claim 5, wherein the data identifying said parameters represents the type and/or format and/or description of said data values.

7. A method according to claim 5 or 6, further comprising the step of providing a second computer code to said second computer, wherein said second computer code is adapted to encrypt data supplied by said second computer.

8. A method of monitoring website activity in a network of interconnected computers, the method substantially as hereinbefore described with reference to the accompanying drawing.

9. A computer program product comprising:-

a first computer code to be supplied by a first computer and adapted to define a set of data parameters, the values of which are to be acquired from a second computer; and

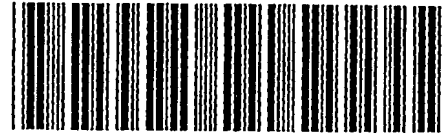a second computer code defining data identifying said parameters;

wherein said first and second computer codes are adapted to be supplied to said second computer in response to a request from said second computer for web page data from said first computer

and to provide said data values together with said data identifying said parameters to a third computer.

10. A computer program product according to claim 9, further comprising a third computer code adapted to encrypt data sent from said second computer.

Internet

Fig. 1

THIS PAGE BLANK (USPTO)